View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Siberian Federal University Digital Repository

УДК 004.946

РАЗРАБОТКА И ИСПОЛЬЗОВАНИЕ УНИВЕРСАЛЬНОЙ СТРАТЕГИИ ЗАЩИТЫ ВИРТУАЛЬНЫХ ИНФРАСТРУКТУР

Угрюмов Д.В.

Научный руководитель – доцент Осипенко Л.П.

Кубанский государственный технологический университет

В настоящее время технология виртуализации является одной из наиболее перспективных и быстро развивающихся. Это связано с тем, что внедрение подобной технологии позволяет снизить затраты на информационную инфраструктуру, повысить гибкость управления, обеспечить высокую надежность работы приложений при сбоях, а также добиться экономии энергии и площади серверных помещений.

Стоит отметить, что наряду с преимуществами виртуализации появляются и дополнительные проблемы информационной безопасности, которые тоже требуется решать. По этой причине следует уделить значительное внимание проблеме несанкционированного доступа (далее – НСД) вредоносных программ к ресурсам виртуальных информационных систем, а также опасных действий злоумышленников.

Таким образом, возникают актуальные вопросы информационной безопасности:

1. Как определить корректность создания, клонирования, перемещения виртуальных машин?
2. Каким образом обезопасить виртуальную инфраструктуру от атак на её клиентские компоненты?
3. Как избежать неконтролируемого роста количества виртуальных машин?
4. Каким образом защитить средства управления и администрирования виртуальной инфраструктурой?

Так как рассматриваемая среда представляет собой дополнительный программно-аппаратный уровень, то любое изменение архитектуры и появление новых компонентов ведет и к появлению новых угроз. Для разработки эффективной стратегии защиты виртуальных систем требуется, в первую очередь, классифицировать возможные угрозы:

1. Атака на гипервизор. Следует отметить, что вредоносное ПО может получить НСД к серверу виртуализации, гипервизору и средствам администрирования вследствие того, что сам сервер виртуализации может содержать уязвимости и ошибки конфигурирования.
2. Атака на жёсткий диск виртуальной машины: виртуальная машина обычно запущена на сервере виртуализации, а ее жёсткий диск хранится на определённом носителе. Злоумышленник может изменять и копировать данные на дисках виртуальных машин, даже когда они выключены и не функционируют, без участия программного обеспечения данных машин.
3. Атака на средства управления виртуальной машиной: при получении НСД вредоносного ПО к средствам администрирования, возникают риски хищения или модифицирования данных в виртуальной инфраструктуре.
4. Атака на одну виртуальную машину с другой виртуальной машины: виртуальные машины одного физического сервера могут обмениваться трафиком

напрямую, минуя физические коммутаторы, следовательно, использование физических межсетевых экранов неэффективно.

5. Атака на сеть репликации виртуальных машин: с помощью сети репликации передаются сегменты оперативной памяти виртуальных серверов, значит, существует риск перехвата таких данных. Также злоумышленник может копировать, изменять и блокировать поток данных, идущий на все устройства: накопители, периферийное оборудование.

6. Бесконтрольный рост количества виртуальных машин: динамичность, одна из основных особенностей виртуальной среды является как достоинством, позволяющим быстро выполнять развертывание и миграцию виртуальных машин, так и недостатком системы безопасности, если к виртуальным машинам не применяются политики безопасности.

Далее следует рассмотреть возможные способы выявления нарушений безопасности в виртуальной инфраструктуре. Главной особенностью при выявлении нарушений в виртуальной среде является то, что в ней нельзя полагаться на стандартные механизмы ведения журналов и аудита операционных систем и приложений. Для выявления фактов НСД необходимо осуществлять мониторинг и аудит следующих уровней:

1. Гипервизора на уровне его операционной системы. Системные события являются низкоуровневыми и их нельзя связать с действиями на уровне виртуализации (копирование, изменение, перемещение виртуальных машин), но это необходимо для выявления аппаратных и программных сбоев, незапланированных перезагрузок физических хост-серверов и т.д.
2. Мониторинг уровня виртуализации. На данном уровне происходят наиболее важные событий с точки зрения защиты информации. Следует отметить, что не все системы мониторинга способны следить за данным уровнем.
3. Мониторинг событий гостевой операционной системы и приложений.
4. Мониторинг событий физической инфраструктуры, обслуживающей виртуальные сервера.

Помимо мониторинга и аудита, нужно также использовать правила выявления узкоспециализированных инцидентов, присущих виртуальной инфраструктуре, используя систему корреляции событий информационной безопасности (далее - Security Information and Event Management, SIEM-система). Данные системы выполняют важные функции: сбор сигналов тревоги от различных средств защиты, анализ их, поиск скрытых зависимостей и пропущенных отдельными средствами защиты информации (далее – СЗИ) атак, и рекомендация определённых корректирующих воздействий.

Далее следует проанализировать особенности применения стандартных подходов и средств для защиты компонентов виртуальных инфраструктур.

Рассмотрим обеспечение безопасности на сетевом уровне. Как было сказано ранее, траффик между двумя виртуальными машинами, находящимися на одном хосте, не покидает его, следовательно, он не проходит через межсетевой экран. Ошибочно полагать, что данная угроза актуальна, только в пределах одного хостового сервера. Представим ситуацию, когда сначала скомпрометированная машина получит контроль над остальными виртуальными машинами на своём хосте, а дальше, при миграции на другой хост, компрометация будет распространяться далее.

Следующей важной особенностью виртуальных инфраструктур является то, что нельзя полагаться только на статические правила на коммутаторах. В физическом мире

непривычной является ситуация, когда серверы могут менять физические порты, тогда как в виртуальной структуре в процессе миграции такая ситуация стандартна.

Тем не менее, использование межсетевых экранов (далее – МЭ) позволяет уменьшить количество атакуемых виртуальных серверов, а также предоставляет следующие возможности: изоляцию виртуальной машины внутри сетевого сегмента; фильтрацию траффика; анализ протоколов; предотвращение атак типа DoS; внедрение политик безопасности; сканирование сетевого окружения на виртуальных серверах.

Рассмотрим применение Систем Обнаружения и Предотвращения Вторжений для экранирования уязвимостей операционных систем и приложений до установки обновлений безопасности. Внедрение подобных систем на виртуальных машинах позволяет обеспечить достаточный уровень защиты от атак, направленных на некоторые известные уязвимости без установки обновлений, а также блокировать атаки типа XSS (межсайтовый скриптинг) и SQL Injection.

Важно отметить необходимость применения подсистемы контроля целостности, которая позволяет выявлять изменения, возникающие вследствие компрометации системы вредоносным ПО. Данная подсистема выполняет следующие функции: проверку по запросу или по расписанию; контроль атрибутов файлов, их свойств; контроль на уровне каталогов; настройку объектов контроля; составление отчетов.

Необходимо также осуществлять анализ журналов, включающий сбор и просмотр журналов работы операционных систем и приложений, что позволяет выявлять события нарушения безопасности во всём массиве записей: подозрительное поведение пользователей и процессов; мониторинг действий администратора безопасности; сбор событий с физических, и виртуальных серверов.

Крайне важно и применение специализированных средств защиты от вредоносных программ, учитывающих особенности виртуализации благодаря специальным программным интерфейсам гипервизора, которые позволяют проводить сканирование в реальном времени, обеспечиваемое антивирусным агентом внутри виртуальной машины, и сканирование виртуальных машин целиком на уровне гипервизора, что гарантирует безопасность даже выключенной виртуальной машины. Подобный подход позволяет защититься от вредоносных программ, блокирующих работу антивируса.

Одним из наиболее перспективных и современных направлений в обеспечении безопасности виртуальных инфраструктур является технология создания зон безопасности. Зона безопасности представляет собой совокупность ресурсов, которые подвержены некоторым общим рискам безопасности. При построении подобных зон для защиты виртуальных инфраструктур нужно учитывать следующие правила:

1. Все компоненты одной зоны безопасности подвержены одним рискам.
2. Все компоненты одной зоны безопасности имеют равную ценность.
3. Компоненты, граничащие с интернетом, никогда не располагаются в сети, где находятся компоненты, не граничащие с ним.
4. Взлом одной зоны не должен вести к взлому другой зоны.
5. Зоны безопасности нужно выделять с помощью физической либо логической сегментации; необходимо обеспечить минимальные привилегии доступа устройств различных зон друг к другу.

Далее рассмотрим направления в обеспечении безопасности конкретных компонентов виртуальной инфраструктуры.

При атаке на гипервизор следует применять следующие меры защиты:

1. Установка прав доступа к физическому серверу виртуализации.
2. Своевременная установка обновлений безопасности для программного обеспечения среды виртуализации.
3. Ограничение прав на запуск программ.

При атаке на средства управления виртуальной машиной следует использовать защиту периметра сети путем разграничения доступа к серверам виртуальных машин и средствам управления инфраструктуры. Защита достигается комплексом организационных и технических мер, среди которых: отделение сети администрирования виртуальной инфраструктуры с последующей защитой периметра данной сети. Необходим также контроль целостности и доверенная загрузка хост-серверов виртуализации; ограничение физического доступа к серверам; своевременная установка обновлений безопасности для ПО виртуализации и ряд дополнительных мер.

При атаке на жёсткий диск виртуальной машины нужно обеспечить защиту обрабатываемой информации виртуальных машин путём разграничения доступа к файлам дисков виртуальных машин.

Для защиты от атак на одну виртуальную машину с другой виртуальной машины требуется использование специализированных МЭ, которые могут использоваться в виртуальной среде.

Для защиты от атак на сеть репликации виртуальных машин необходимо изолировать сеть репликации от остальных сетей, либо использовать средства построения виртуальных частных сетей VPN для канала репликации.

Для предотвращения бесконтрольного роста числа виртуальных машин требуется организация централизованного процесса управления жизненным циклом виртуальных машин, согласованного с политикой безопасности организации.

Так как технология виртуализации только набирает обороты и стремительно развивается, то необходима единая стратегия обеспечения безопасности, обеспечивающая надёжную защиту от новых видов угроз. Ситуацию осложняет отсутствие на сегодняшний день в Российской Федерации официальных стандартов и иных руководящих документов, описывающих особенности построения и организации защиты виртуальных инфраструктур.

Следует отметить, что задача обеспечения достаточного уровня информационной безопасности в средах виртуализации осуществима и реализуется посредством следующих действий: разработка внутренних политик безопасности, следование рекомендациям экспертов, использование специализированных решений.

В результате разработки стратегии защиты можно сделать следующие выводы:

1. В виртуальной инфраструктуре нужно применять новые СЗИ, учитывающие особенности обеспечения безопасности сред виртуализации.
2. Большинство традиционных аппаратных средств защиты будут некорректно работать в виртуальной среде.

3. Новые компоненты инфраструктуры: гипервизор, средства управления виртуальной инфраструктурой также надо защищать.
4. При организации защиты, помимо специализированных мер, необходимо применять и стандартные меры обеспечения безопасности физических инфраструктур, только используя комплексный подход, можно быть уверенным в надёжной защите виртуальных ресурсов.

Следовательно, разработанная стратегия защиты является крайне актуальной, а результаты реализации стратегии качественным образом повысят уровень безопасности виртуальных сред предприятий и организаций.